Name:Douglas Sweeting

Class:WDD345-O

Date: 8/19/14

1. What type of log file is it?
   1. Error log file, Access log files, one message log files and one secure log file.
2. What are the dates which are represented by the logs?
   1. Nov 10thth – Dec 10th Error\_Log
3. How many unique users appear?
   1. 11+
4. What was the largest data export? and does it look out of the ordinary?

66.249.76.146 - - [09/Dec/2013:16:48:38 +0000] "GET /sites/default/files/images/Bonenfont.png HTTP/1.1" 200 87498 "-" "Googlebot-Image/1.0" – No because this appears to be an image.

1. What is the most common error found in the error logs?
   1. Script not found and file not found.
2. Do you see anything which is out of the ordinary?
   1. Yes, IP address 202.107.225.31 and 42.96.129.148 (both from China) tried to log in unsuccessfully. A Lot. Not only that, but when trying to log in with 42.96.129.148, they were port knocking as well. Also, I don’t know, but it looks like whomever it was may have found Mr. Dalton’s username and tried to use it at the end but logged in with the wrong password.
3. Write a short synopsis of what you found in each file.
   * 1. Excluding error\_log\_20131124 most of the error messages were script not found errors coupled with file not found errors. Those were the most common errors found. There were a lot of log in attempts that failed as well. Also, there was a bug in the server as well which caused a backtace to be done.